FREEDMAN & Associates
REGISTERED PATENT AND TRADEMARK AGENTS

Gordon Freedman, LLB, Patent* and Trademark Agent
Computer and Systems Engineer

Juergen Fuchs, Ph.D. Mech.Eng.

Anne Decrouy, Ph.D. Physiol.

Mark R. Weir, Ph.D. Chem.

* Registered in Canada and U.S.

117 Centrepointe Drive, Suite 350
Nepean, Ontario
Canada K2G 5X3
Tel (613) 274-7272
Fax (613) 274-7414

Email· gordon@ipatent4u.com
http://www ipatent4u.com

August 31, 2000

The Commissioner of Patents and Trademarks
Washington, D.C. 20231
U.S.A.

Sir:

Re: New United States Patent Application
      Inventor(s):   Hamid et al.
      Title: FLEXIBLE METHOD OF SECURITY DATA BACKUP
      Our File: 12-51 US

Enclosed for the filing of a new patent application in the United States are:

1. Small Entity form – completed;
2. Declaration signed by the Inventor(s);
3. **23** pages of specification, **44** claims, **3** being independent; Abstract of the Disclosure;
4. Formal drawings including **9** figures;
5. A cheque in the sum of **$561.00** to cover the filing fee.

We will be pleased to receive the filing particulars of this application. Enclosed is a self-addressed return postcard to indicate that the application has been received by the USPTO.

Please charge any additional fees or credit overpayment to Deposit Account No: 50-1142.

Respectfully submitted,

Gordon Freedman
Regn. No. 41,553

VERIFIED STATEMENT CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) & 1.27(c))-SMALL BUSINESS CONCERN	Attorney Docket No. 12-51 US

Applicant or Patentee: **LAURENCE HAMID AND ROBERT D. HILLHOUSE**

Serial or Patent No:

Filed or Issued:

Title: **FLEXIBLE METHOD OF SECURITY DATA BACKUP**

I hereby declare that I am
[   ] the owner of the small business concern identified below:
[X] an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF SMALL BUSINESS CONCERN   **Dew Engineering and Development Limited**

ADDRESS OF SMALL BUSINESS CONCERN   **3429 Hawthorne Road, Ottawa, Ontario, Canada K1G 4G2**

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.12, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, described in:

          [X]   the specification filed herewith with title as listed above.
          [   ]   the application identified above
          [   ]   the patent identified above.

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention must file separate verified statements averring to their status as small entities and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern or organization having any rights in the invention is listed below:

          [X]   No such person, concern, or organization exists.
          [   ]   Each such person, concern, or organization is listed below.

Separate verified statements are required from each named person, concern organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28 (b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such wilful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING   W. R. ROUECHE

TITLE OF PERSON IF OTHER THAN OWNER   PRESIDENT

ADDRESS OF PERSON SIGNING   **3429 Hawthorne Road, Ottawa, Ontario, Canada K1G 4G2**

SIGNATURE _____ DATE ___16 W/March 2000___

Flexible Method of Security Data Backup

Field of the Invention

This invention relates generally to authorization of individuals and more particularly relates to a method of storing security data in a secure and retrievable

5   fashion.

Background of the Invention

Computer security is fast becoming an important issue. With the proliferation of computers and computer networks into all aspects of business and daily life - financial, medical, education, government, and communications - the concern over secure file

10   access is growing. Using passwords is a common method of providing security. Password protection and/or combination type locks are employed for computer network security, automatic teller machines, telephone banking, calling cards, telephone answering services, houses, and safes. These systems generally require the knowledge of an entry code that has been selected by a user or has been preset.

15   Preset codes are often forgotten, as users have no reliable method of remembering them. Writing down the codes and storing them in close proximity to an access control device (i.e. the combination lock) results in a secure access control system with a very insecure code. Alternatively, the nuisance of trying several code variations renders the access control system more of a problem than a solution.

20   Password systems are known to suffer from other disadvantages as well. In most cases, a user specifies the password . Most users, being unsophisticated users of security systems, choose passwords that have a personal connection or significance; this practice makes the password not only easy to remember but also relatively insecure. As such, many systems that rely solely on password protection are easily accessed by an

25   unauthorized third party through a simple trial and error process.

A security access system that provides substantially secure access and does not require a password or access code is a biometric identification system. A biometric

1

identification system accepts unique biometric information from a user and identifies the user by matching the information against information belonging to registered users of the system. One such biometric identification system is a fingerprint recognition system. In this type of system, the finger under investigation is usually pressed against a flat surface,

5   such as a side of a glass plate; the ridge and valley pattern of the fingertip is sensed by a sensing means such as an interrogating light beam. Fingerprint identification devices of this nature are routinely used to control the building-access or information-access of individuals to buildings, rooms, and devices such as computer terminals.

Various optical devices are known which employ prisms upon which a finger whose print is to be identified is placed. The prism has a first surface upon which a finger is placed,

10   a second surface disposed at some angle to the first surface through which the fingerprint is viewed and a third illumination surface through which light is directed into the prism. In some cases, the illumination surface is at an acute angle to the first surface, as seen for example, in US Patents 5,187,482 and 5,187,748. In other cases, the illumination surface is

15   parallel to the first surface, as seen for example, in US Patents 5,109,427 and 5,233,404.

United States patent number 4,353,056 in the name of Tsikos issued October 5, 1982, discloses an alternative kind of fingerprint sensor that uses a capacitive sensing approach. The described sensor has a two-dimensional, row and column, array of capacitors, each comprising a pair of spaced electrodes, carried in a sensing member and covered by an

20   insulating film. The sensors rely upon deformation to the sensing member caused by a finger being placed thereon so as to vary locally the spacing between capacitor electrodes, according to the ridge/trough pattern of the fingerprint, and hence, the capacitance of the capacitors. In one arrangement, the capacitors of each column are connected in series with the columns of capacitors connected in parallel and a voltage is applied across the columns.

25   In another arrangement, a voltage is applied to each individual capacitor in the array. Sensing in the respective two arrangements is accomplished by detecting the change of voltage distribution in the series connected capacitors or by measuring the voltage values of the individual capacitances resulting from local deformation. To achieve this, an individual connection is required from the detection circuit to each capacitor.

The analysis of fingerprints is discussed in the following references, which are hereby incorporated by reference:

Xiao Qinghan and Bian Zhaoqi,: An approach to Fingerprint Identification By Using the Attributes of Feature Lines of Fingerprint," IEEE Pattern Recognition, pp 663, 1986;

5   C.B. Shelman, " Fingerprint Classification - Theory and Application," Proc. 76 Carnahan Conference on Electronic Crime Countermeasures, 1976;

Feri Pernus, Stanko Kovacic, and Ludvik Gyergyek, "Minutaie Based Fingerprint Registration," IEEE Pattern Recognition, pp 1380, 1980;

J.A. Ratkovic, F.W. Blackwell, and H.H. Bailey, "Concepts for a Next Generation

10   Automated Fingerprint System," Proc. 78 Carnahan Conference on Electronic Crime Countermeasures, 1978;

K. Millard, " An approach to the Automatic Retrieval of Latent Fingerprints," Proc. 75 Carnahan Conference on Electronic Crime Countermeasures, 1975;

Moayer and K.S. Fu, "A Syntactic Approach to Fingerprint Pattern Recognition," Memo

15   Np. 73-18, Purdue University, School of Electrical Engineering, 1973;

Wegstein, *An Automated Fingerprint Identification System*, NBS special publication, U.S. Department of Commerce/National Bureau of Standards, ISSN 0083-1883; no. 500-89, 1982;

Moenssens, Andre A., Fingerprint Techniques, Chilton Book Co., 1971; and,

20   Wegstein and J.F. Rafferty, *The LX39 Latent Fingerprint Matcher*, NBS special publication, U.S. Department of Commerce/National Bureau of Standards; no. 500-36, 1978.

Although biometric authentication is a secure means of identifying a user, it has not penetrated the marketplace sufficiently to be on most desktops. Further, since most

25   forms of biometric authentication require specialised hardware, market penetration is slow and requires both acceptance of the new hardware and a pressing need. The motivation for a company to establish such sophisticated user authentication systems, despite the considerable time and resources that are involved, is the potential that they will incur even greater losses in the event that an unauthorized third party gains access to

30   their secure files.

Secure files are often stored on a computer or network server only in an encrypted form. A user wishing to have access to an encrypted file must first be authenticated as an authorized user of the system. Once the user has been authenticated, a key is provided to the user for the purpose of decrypting the contents of the electronic file and thus allowing

5   the user access to the file.

Key management systems are well known. One such system, by Entrust® Technologies Limited is currently commercially available. Unfortunately, current key management systems are designed for installation on a single computer for use with a single fixed user authorization method and for portability between computers having a

10   same configuration. As such, implementation of enhanced security through installation of biometric input devices is costly and greatly limits portability of key databases. For example, when using Entrust® software to protect a key database, the database is portable on a smart card or on a floppy disk. The portable key database is a duplicate of the existing key database. User authentication for the portable key database is identical to

15   that of the original key database. The implications of this are insignificant when password user authentication is employed; however, when biometric user authentication such as retinal scanning or fingerprint identification are used, the appropriate biometric identification system is required at each location wherein the portable key database is used.

20   To minimize the risk of key compromise the members of an organisation are permitted to travel with limited portable key databases, preferably restricted to the secure keys of a single user.

Another system that is known for key management includes a key-server. A key-server is a single system that provides keys to individuals upon identification or

25   authorization. Such a system is useful in large organisations since it permits changing of system access codes without requiring every user to provide their personal key data storage device. Because of the extreme problems associated with losing secure keys, it is essential that a key-server be backed up appropriately. Further, it is necessary that the key-server be available at all times. This is currently achieved through duplication of key-

servers. Unfortunately, key-servers are costly and this makes their implementation problematic in some instances. For example, a company performing a trial of a new user access system, such a fingerprint identification system, often purchases and installs only a handful of "test" workstations. Thus, to try out ten (10) fingerprint scanners with a key-

5   server configuration requires two robust key-servers having full backup capabilities, a main key-server and a duplicate key-server, and 10 fingerprint imagers. Since a fingerprint imager is likely to cost much less than 10% of the cost of the key-servers, the additional cost is extremely undesirable, dissuading potential customers from performing trials. Eliminating a need for a duplicate key-server would be highly advantageous.

10   Another serious limitation of key management systems configured with a key-server is that individuals do not have access to secure files when they are other than at a workstation in communication with the key-server. Individuals who are required to fly during a business trip may wish to avail themselves of the extra time to edit a report, for example, which is stored on a local hard drive within a portable computer. The electronic

15   file containing the report, however, is stored only in an encrypted form. In order to decrypt the file, the user must first be authenticated by and then receive a key from a key-server. Since a key-server is generally other than accessible when the user is other than at work, the user's ability to perform tasks from remote locations is greatly reduced. It would be advantageous to provide a system to allow a user to gain access to a system

20   using a portable key storage device and, as such, have access to a predetermined set of keys both at work and elsewhere.

Object of the Invention

In an attempt to overcome these and other limitations of the prior art, it is an object of this invention to provide a method of backing-up the secure key information

25   stored on a main key-server without a need for a second duplicate key-server.

Summary of the Invention

According to this method, the secure key database that is stored on an organizations main key-server is backed-up in a distributed fashion. Each user carries

with them only that part of the whole database that is related specifically to that user. Since the portable data storage device contains only those secure keys that are assigned to and associated with one specific user, only a small number of secure keys may be compromised in the event that a single portable data storage device is lost. Further, when

5   the personal data storage device is in the form of a token, the secure keys stored internal to the token in non-volatile memory means and are not accessible outside the module. The keys cannot be viewed or extracted from the token in the event that it is lost, thus providing additional security.

In accordance with the invention there is provided a method of restoring data of a

10   key-server in communication with a communication network comprising the steps of: providing the key-server in communication with the communication network; providing to at least a computer in communication with the communication network, a plurality of portable data storage devices each having stored thereon security data relating to a single authorized user; copying from each of the plurality of portable data storage devices,

15   security data relating to the single authorized user.

In accordance with the invention there is also provided a method of backing up data of a key-server in communication with a communication network comprising the steps of: providing the key-server in communication with the communication network,

20   the key-server having stored thereon the unique user identification information for a plurality of authorized users of the communication network and the security data for use by the specific authorized user in accessing data within the network; providing to at least a computer in communication with the communication network, a portable data storage device; receiving user identification data indicative of an authorized user of the

25   communication network; and, copying from the key-server to the portable data storage device, security data relating to the authorized user for use by the specific authorized user in accessing data within the network.

In accordance with the invention there is further provided a method of

30   authenticating an individual for allowing access to secure data or secure keys stored on a communication network when other than in communication with a central key-server

comprising the steps of: providing at least a computer in communication with the communication network; determining at least an available user information entry device from a plurality of known user information entry devices; determining the availability of one of a key-server and a portable data storage device in communication with the

5   computer; receiving user identification information via the at least an available user information entry device; authenticating the individual for access to at least one of the secure data and secure keys stored on the determined one of a key-server and a portable data storage device.

10   It is an advantage of the present invention that a user can gain access to a system using a portable key storage device and, as such, has access to a predetermined set of keys both at work and elsewhere. It is a further advantage that the portable key storage device acts as a data backup for a portion of the keys within the key-server thus eliminating a need to have a duplicate key-server.

15   It is another advantage of the present invention that the keys stored on the key-server and on the portable backup are secured against access by individuals and that security is maintainable even when copying keys.

Brief Description of the Drawings

An exemplary embodiment of the invention will now be described in conjunction

20   with the attached drawings, in which:

Fig. 1a is a simplified block diagram of a prior art method of storing key data on a main key-server and of storing backup key data on a duplicate key-server is shown.

Fig. 1b is a simplified block diagram of a prior art method of Fig. 1a, in which the duplicate key-server has been activated following a crash of the main key-server, is

25   shown

Fig. 2 is a simplified block diagram of another prior art method of storing key data on a users system without backup key data is shown.

Fig. 3 is a simplified block diagram of yet another prior art method of storing key data on a users system with backup key data stored on floppy disks is shown.

Fig. 4 is a method according to the invention of storing key data on a key-server with distributed backup key data stored remotely absent a second key-server is shown.

5   Fig. 5 is a simplified flow diagram of a method implemented upon key-server failure is shown.

Fig. 6a is a simplified flow diagram of a method of user authorization making use of security data stored on a portable data storage device is shown.

Fig. 6b is a simplified flow diagram of a method of user authorization making use of
10   security data stored on a locally available key-server is shown.

Fig. 7 is a simplified flow diagram of a method of replacing a portable data storage device is shown.

Detailed Description of the Invention

The invention is described with respect to passwords, tokens, and biometric
15   verification in the form of fingerprint registration. The method of this invention is applicable to other verification processes as is evident to those of skill in the art.

One of the many problems associated with the use of a fingerprint biometric is that a special contact-imaging device is required to image a fingerprint. Today, many systems and, in particular, many personal computers are not equipped with a contact
20   imaging device. It is well known to outfit a network of workstations with biometric imaging devices in order to overcome these limitations. Unfortunately, for those who travel on business and need access to sensitive data in the form of network data or encrypted email, such a solution is not always possible and convenient. Another known solution is to travel with a portable contact-imaging device. Unfortunately, the cost of
25   purchasing the special software and the additional hardware that are required to implement such a system makes this approach impractical in most cases. Also, many different biometric identification techniques are now known and available. It is

8

impractical to install hardware and software in order to switch between verification methods. According to the invention, a method is proposed for providing a flexible authentication process that maintains security of an overall system without causing undue inconvenience or limitations.

5   One of the many factors slowing widespread introduction of fingerprint-based authentication is the need for key-servers. A key-server is a mission critical system for providing fingerprint authentication data and other security data. Unfortunately, in order to run a trial of a fingerprint security system a main key-server and a duplicate key-server are necessary. Thus, a user is forced to purchase two mission critical quality systems in

10   order to implement a field trial. When the field trial involves of thousands of workstations, it is cost effective. However, when the field trial is, as is more typical, of 10 or 20 workstations, the costs for that trial are excessive.

           Referring to Fig. 1a, a simplified block diagram of a prior art method of storing key data on a main key-server **1** and of storing backup key data on a duplicate key-server

15   **4** is shown. As seen in the block diagram a main key-server **1** is provided with all security data relating to a network **2**. A user wishing to access data on the network **2** via a computer **3** provides user authorization information to the computer **3** using an available user information entry device **5**, which is peripheral to the computer **3**. If the supplied user authorization data matches the user authorization data stored on the key-server, the

20   user is authenticated. The authorization process may occur within the computer **3** based on data retrieved from the main key-server **1** or alternatively may occur on the main key-server **1** using data stored therein. The user now has access to data secured with keys stored on the main key-server **1** and to which the user is provided access. The user information entry device **5** may be a standard keyboard, or alternatively a biometric

25   imaging device such as a fingerprint imager or a retina scanner. Of course, the user information entry device may also comprise any one of a plurality of other known devices, either individually or in combination with at least one other known device, depending upon the level of security that is required for a specific application.

Referring to Fig. 1b, a simplified block diagram of a prior art method of Fig. 1a, in which the duplicate key-server has been activated following a crash of the main key-server, is shown. When the main key-server **1** fails, the duplicate key-server **4** is automatically activated by the action of some electronic switching means **6**, and

5   immediately begins providing identical services to those provided by the main key-server **1**. Using data mirroring techniques, the data within the main key-server **1** and within the duplicate key-server **4** are identical and as such, no data is lost and no interruption to use of the network **2** occurs.

Unfortunately, the prior art systems that require duplicate key-servers are too

10   costly to be implemented for smaller networks. In addition, the complete loss of both the main key-server **1** and the duplicate key-server **4**, for example as the result of a fire, flood, electrical system failure or another similar unforeseeable incident, results in the permanent or temporary loss of the secure key database. Such a catastrophic occurrence will result in the lengthy or even permanent inability of authorized individuals to access

15   secure files etc. on the network.

Referring to Fig. 2, a simplified block diagram of another prior art method of storing key data on a user's computer system, absent backup key data, is shown. Here, a plurality of computers **21** is connected to a network **22**. Each computer has stored thereon, key data specific to a user of that computer. The user logs onto the computer and

20   has access to their key data. Such a system is problematic for many reasons. Firstly, the system is only as secure as each computer. Secondly, there is no central control over keys and access to keys. Thirdly, keys are easily lost during system upgrades or crashes. Fourthly, a user is confined to using a single computer within the network. With today's trends toward mobile offices and so forth, it would be advantageous not to limit users in

25   any of these ways.

Referring to Fig. 3, a simplified block diagram of yet another prior art method of storing key data on a users computer **31** with backup key data stored on floppy disks **33** is shown. Here the chances of losing security data are reduced over those presented with reference to Fig. 2, but not by much. The floppy disks **33** now must be centrally managed

to ensure correct labelling and to ensure that the data is actually backed up according to a regular schedule, and so forth. The use of an insecure medium, such as a computer floppy disk **33**, also renders the backup key data stored thereon more vulnerable to extraction and use by an unauthorized third party.

5   As such, only the system of Fig. 1 meets the security objectives of most business needs. Unfortunately the system of Fig. 1 is too expensive to be implemented on most small-scale networks. In the case of a field trial of a small number of biometric information entry devices, say approximately fifty (50) fingerprint imagers, the cost of purchasing a duplicate key-server is very significant compared to the cost of purchasing

10   the biometrics. Obviously, a method that obviates the need for a duplicate key-server and additionally provides a method for storing a duplicate secure key database would be of great value for use in small-scale networks.

Referring to Fig. 4, a method according to the invention of storing key data on a key-server with distributed backup key data stored remotely on portable data storage

15   devices and absent a duplicate key-server is shown. Here a key-server **41** is shown coupled to a plurality of computers **43**. Each computer **43** has an interface (not shown) for interfacing with a portable data storage device **44** in the form of a token or a smart card. Of course another portable data storage device is also useful, such as a floppy disk.

Within the key-server **41** is stored all security data including user authentication

20   data and secure keys. Each individual also maintains a personal copy of the secure data and of the authentication data within their own portable data storage device **44**. When a user seeks to access the network, they provide their portable data storage device **44** and then authorize themselves. Thus, the functions of key-server **41** are not required by most individuals, such individuals being engaged only in routine activities while at a

25   workplace. Occasionally, individuals may be required to provide their portable data storage device for the transfer of updated or revised security data from the key-server; however, this is not considered a routine activity.

When the user forgets their portable data storage device **44**, the data is available from the key-server **41**. Thus access to the network is still available. When the portable

11

data storage device **44** is lost, it can be reissued by copying the data again from the key-server **41**. Conversely, when the key-server **41** crashes, its data files are rebuilt from each of the portable data storage devices **44**. As such, the need for a backup key-server is obviated. In particular, the use of portable data storage devices **44** for storing personal

5   key data and for use in the authorization and key management functions of security results in a situation wherein use of the key-server **41** is limited to very specific circumstances –lost portable data storage device, forgotten portable data storage device, etc. As long as a portable data storage device isn't lost on the same day as a key-server failure including data loss, all data is recoverable. As such the duplicate key-server is

10   unnecessary. Similarly, when the key-server crashes, only those individuals who are without their portable data storage devices are inconvenienced since everyone else can access the network **42** and their secure keys.

When cryptographic functions are performed within the portable storage devices **44**, the secure keys are not available outside the portable storage devices **44**. Since most

15   cryptographic functions are performed on the portable storage devices **44**, the key-server can support the processing of cryptographic functions for those individuals with forgotten portable storage devices **44**. If a secure path is initiated between portable storage devices **44** and the key-server **41**, then the keys stored within the two media are not available for capture or compromise.

20   Referring to Fig. 5, a simplified flow diagram of a method implemented upon a key-server failure is shown. A portable data storage device containing an individual's security data and authorization information is mated with an interface peripheral to a computer in communication with the key-server. A secure communication session is established from the portable data storage device to the key-server. Security data for an

25   individual user stored within the memory means of the portable data storage device is transferred via the secure communication session to the key-server and stored within the memory means thereon. Since each portable data storage device contains only a portion of the original secure key database that existed on the key-server, it is necessary to repeat this procedure for every individual's portable data storage device. Once all of the secure

key data has been transferred from the portable data storage devices, the original database is essentially completely reconstructed and normal key-server functions resume.

5

10

15

20

Referring to Fig. 6a, a simplified flow diagram of a method of user authorization making use of security data stored on a portable data storage device is shown. Authorization making use of a portable data storage device is likely to occur when the user is other than in the workplace, for example during times of travel or when working from a home office or other remote location. Of course, the portable data storage device is used in the workplace as well, especially when the functions of the key-server are limited to specific instances as was previously described. The user wishing to obtain authorization for access to secure keys or files on the network provides their portable data storage device, in the form of a smart card or a token, containing personal security information including authentication methods at a computer in communication with a communication network. The presence of available user information entry devices in communication with the computer, from a plurality of user information entry devices, is determined. The user provides data via at least an available user information entry device. This could involve entering a password via a standard computer keyboard, or providing biometric data such as a fingerprint using an available fingerprint imaging station. The data provided by the user is registered against known data for that user, stored in the portable data storage device. If the data provided by the user matches the data stored in the portable storage device, the user is authorized for access to selected secure keys and secure files.

25

30

Referring to Fig. 6b, a simplified flow diagram of a method of user authorization making use of security data stored on a key-server is shown. Authorization making use of security data stored on a key-server would typically occur only in instances when an individual has lost or forgotten their portable data storage device. The presence of available user information entry devices in communication with a computer in communication with a communication network, from a plurality of user information entry devices, is determined. The user provides data via at least an available user information entry device. This could involve entering a password via a standard computer keyboard, or providing biometric data such as a fingerprint using an available fingerprint imaging

station. The data provided by the user is registered against known data for that user, which is stored on the key-server. If the data provided by the user matches the data stored in the key-server, the user is authorized for access to selected secure keys and secure data files. Alternatively, the user is authorised for access to selected key-server functions in

5   the form of cryptographic functions.

Referring to Fig. 7, a simplified flow diagram of a method of replacing a portable data storage device is shown. This procedure is performed, for example, in the event that a user has permanently lost their original portable storage device containing their personal security information. A blank portable data storage device, in the form of a

10   smart card or token, is inserted into an interface peripheral to a computer in communication with a communication with a network. The interface includes a means for writing data to the portable data storage device. A secure communication session is established from the portable data storage device to the key-server. Secure key data, specific to an individual user, is transferred from the key-server to the portable data

15   storage device via the secure communication session. The transferred secure key data is stored within the memory means of the portable data storage device. The portable data storage device, containing the transferred personal security data, is removed from the interface peripheral to the computer in communication with a network and can be used for the purpose of authorizing the user.

20   Numerous other embodiments may be envisaged without departing from the spirit and scope of the invention.

Claims

What is claimed is:

1. A method of restoring data of a key-server in communication with a communication
5   network comprising the steps of:
       providing the key-server in communication with the communication network;
       providing to at least a computer in communication with the communication network, a
       plurality of portable data storage devices each having stored thereon security data relating
       to a single authorized user;
10   copying from each of the plurality of portable data storage devices, security data relating
       to the single authorized user.

2. A method of restoring data of a key-server in communication with a communication
   network as defined in claim 1 wherein the step of copying comprises the steps of:
15   forming a secure communication session between at least one of the plurality of portable
       data storage devices and the key-server;
       transferring the security data via the secure communication session from the portable data
       storage device to the key-server; and,
       storing the transferred security data within memory means of the key-server.
20

3. A method of restoring data of a key-server in communication with a communication
   network as defined in claim 2 wherein the plurality of portable data storage devices
   comprise all the security data to be restored in the key-server.

25   4. A method of restoring data of a key-server in communication with a communication
       network as defined in claim 3 wherein the plurality of portable data storage devices
       includes memory having stored therein security data relating to each single authorized
       user of the communication network.

30   5. A method of restoring data of a key-server in communication with a communication
       network as defined in claim 2 wherein the portable data storage device includes a

processor for ciphering data using the security data stored therein and comprising the steps of:

providing cryptographic functions within the portable data storage device using the security data stored therein.

5

6. A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the key-server includes a processor for ciphering data using the security data stored therein and comprising the steps of:

providing cryptographic functions within the key-server using the security data stored

10 therein.

7. A method of restoring data of a key-server in communication with a communication network as defined in claim 6 comprising the steps of:

determining at least an available user information entry device from a plurality of known

15 user information entry devices;

receiving unique user identification information via the at least an available user information entry device; and,

registering the received user identification information against security data for that user stored in the key-server;

20 wherein, when the user identification information is indicative of an authorized user the step of ciphering data is performed with security data associated with the authorized user.

8. A method of restoring data of a key-server in communication with a communication network as defined in claim 3 wherein each of the plurality of portable data storage

25 devices are provided at each of a plurality of computers in communication with the network.

9. A method of restoring data of a key-server in communication with a communication network as defined in claim 8 wherein the portable data storage device is one of a token

30 and a smart card.

10. A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the portable data storage device is one of a token and a smart card.

5   11. A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein at least a portable data storage device provides dedicated cryptographic functions for the at least a computer in communication with the communication network using the security data stored internal to the at least a portable data storage device.

10

12. A method of restoring data of a key-server in communication with a communication network as defined in claim 11 wherein the security data stored internal to the at least a portable data storage device are not accessible in a useable form from outside of the key-server and the at least a portable data storage device.

15

13. A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the key-server provides dedicated cryptographic functions for the at least a computer in communication with the communication network using the security data stored internal to the key-server.

20

14. A method of backing up data of a key-server in communication with a communication network comprising the steps of:

providing the key-server in communication with the communication network, the key-server having stored thereon the unique user identification information for a plurality of

25   authorized users of the communication network and the security data for use by the specific authorized user in accessing data within the network;

providing to at least a computer in communication with the communication network, a portable data storage device;

receiving user identification data indicative of an authorized user of the communication

30   network; and,

copying from the key-server to the portable data storage device, security data relating to the authorized user for use by the specific authorized user in accessing data within the network.

5   15. A method of backing up data of a key-server in communication with a communication network as defined in claim 14 wherein the step of copying comprises the steps of:

forming a secure communication session between the key-server and the portable data storage device;

10   transferring the security data relating to a specific authorized user via the secure communication session from the key-server to the portable data storage device assigned to that specific authorized user; and,

storing the transferred security data relating to a specific authorized user within the memory means of the portable data storage device.

15

16. A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein security data specific to each of a plurality of authorized users of the communication network is stored on a separate portable data storage device assigned uniquely to one of the plurality of authorized users,

20   wherein the security data of the key-server is partially stored within each portable data storage device and wherein all data within the plurality of portable data storage devices is sufficient to restore security data to the key-server in the event of a data loss thereto.

17. A method of backing up data of a key-server in communication with a

25   communication network as defined in claim 15 wherein the portable data storage device includes a processor for ciphering data using the security data stored therein and comprising the steps of:

providing cryptographic functions within the portable data storage device using the security data stored therein.

30

18. A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the key-server includes a processor for ciphering data using the security data stored therein and comprising the steps of:

5   providing cryptographic functions within the key-server using the security data stored therein.

19. A method of backing up data of a key-server in communication with a communication network as defined in claim 18 comprising the steps of:

10   determining at least an available user information entry device from a plurality of known user information entry devices;

receiving unique user identification information via the at least an available user information entry device; and,

registering the received user identification information against security data for that user

15   stored in the key-server,

wherein, when the user identification information is indicative of an authorized user, the step of ciphering data is performed with security data associated with the authorized user.

20. A method of backing up data of a key-server in communication with a

20   communication network as defined in claim 16 wherein each of the plurality of portable data storage devices are provided at each of a plurality of computers in communication with the network.

21. A method of backing up data of a key-server in communication with a

25   communication network as defined in claim 20 wherein the portable storage device is one of a smart card and a PCMCIA token.

22. A method of backing up data of a key-server in communication with a communication network as defined in claim 16 wherein the portable storage device is one

30   of a smart card and a PCMCIA token.

23. A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the portable data storage device provides dedicated cryptographic functions for the at least a computer in communication with the communication network using security data stored internal to the portable data

5   storage device.

24. A method of backing up data of a key-server in communication with a communication network as defined in claim 23 wherein the security data stored internal to the portable data storage device are not accessible from outside of the key-server and

10   the portable data storage device.

25. A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the key-server provides dedicated cryptographic functions for the at least a computer in communication with the

15   communication network using security data stored internal to the key-server.

26. A method of backing up data of a key-server in communication with a communication network as defined in claim 25 wherein the security data stored internal to the key-server are not accessible in a useable from outside of the key-server and the

20   portable data storage device.

27. A method of authenticating an individual for allowing access to secure data or secure keys stored on a communication network when other than in communication with a central key-server comprising the steps of:

25   providing at least a computer in communication with the communication network;
     determining at least an available user information entry device from a plurality of known user information entry devices;
     determining the availability of one of a key-server and a portable data storage device in communication with the computer;

30   receiving user identification information via the at least an available user information entry device;

20

authenticating the individual for access to at least one of the secure data and secure keys stored on the determined one of a key-server and a portable data storage device.

28. A method as defined in claim 27 wherein when a portable data storage device is

5   present the determined one of a key-server and a portable data storage device is the portable data storage device and the received user identification information is registered against user identification information stored in the memory means of the portable data storage device.

10   29. A method as defined in claim 28 comprising the steps of:
receiving unique user identification information via the at least an available user information entry device;
registering the received user identification information against security data for that user stored in the portable data storage device; and,

15   providing secure keys to the user to allow access to encrypted data files that the user has been authenticated to access.

30. A method as defined in claim 28 comprising the steps of:
receiving unique user identification information via the at least an available user

20   information entry device;
registering the received user identification information against security data for that user stored in the portable data storage device; and,
providing cryptographic functions within the portable data storage device using the secure keys associated with the authenticated user.

25

31. A method as defined in claim 28 wherein when a portable data storage device is other than present prompting the user to provide a portable data storage device.

32. A method as defined in claim 28 wherein other than when the user provides a

30   portable data storage device a key-server in communication with the communication network is the determined one of a key-server and a portable data storage device.

21

33. A method as defined in claim 32 comprising the steps of:

receiving unique user identification information via the at least an available user information entry device;

5   registering the received user identification information against security data for that user stored in the key-server; and,

providing secure keys to the user to allow access to encrypted data files that the user has been authenticated to access.

10   34. A method as defined in claim 32 comprising the steps of:

receiving unique user identification information via the at least an available user information entry device;

registering the received user identification information against security data for that user stored in the key-server; and,

15   providing cryptographic functions within the key-server using the secure keys associated with the authenticated user.

35. A method as defined in claim 31 wherein the portable data storage device is one of a smart card and a PCMCIA token

20

36. A method as defined in claim 35 wherein the portable data storage device in the form of a PCMCIA token provides dedicated cryptographic functions for the computer using security data stored internal to the PCMCIA token.

25   37. A method as defined in claim 36 wherein the security data stored internal to the PCMCIA token are not accessible from outside of the PCMCIA token and therefore cannot be extracted or otherwise read by an unauthorized third party.

38. A method as defined in claim 32 wherein the user information entry device is a

30   biometric information entry device.

39. A method as defined in claim 31 wherein a portable data storage device is used to provide an individual with access to a predetermined set of keys in a plurality of different locations.

5   40. A method as defined in claim 39 wherein the method of user authentication required at work is other than the method of user authentication required elsewhere.

41. A method as defined in claim 27 wherein the portable data storage device provides dedicated cryptographic functions for the computer using security data stored internal to

10   the portable data storage device.

42. A method as defined in claim 41 wherein the security data stored internal to the portable data storage device are not accessible in a useable from outside of the key-server and the portable data storage devices.

15

43. A method as defined in claim 27 wherein the key-server provides dedicated cryptographic functions for the computer using security data stored internal to the key-server.

20   44. A method as defined in claim 43 wherein the security data stored internal to the key-server are not accessible from outside of the key-server and the portable data storage devices.

Abstract of the Invention

A method of supporting a substantially secure backup copy of a key-server database, said database comprising security information specific to a plurality of users, absent the need for a duplicate key-server is disclosed. According to the method, each

5   individual's security data is stored within the key-server database and is also stored on a portable data storage device, such as a smart card or a PCMCIA token. If the key-server crashes and the database stored thereon is lost, a duplicate key-server database is reconstructed using the aggregate of the partial database files stored on each individual's portable data storage device. Similarly, when a portable data storage device is lost, it can

10   be rebuilt from the data stored within the key-server.

1

Fig. 1a

Fig. 1b

Fig. 2

Fig. 3

41 〜

42

44 43   44 43   44 43   44 43

Fig. 4

insert portable storage device containing
security data at a computer in
communication with a network

establish secure communication
session from the portable storage
device to the key-server

transfer security data via the secure
communication session from the portable
storage device to the key-server

store the transferred security data within
the reconstructed database of the key-server

data transferred
from all portable
storage devices?

No

Yes

reconstruct the original key-server database
using the composite security data transferred
from individual portable storage devices

resume normal operation
of key-server using reconstructed
security data database

Fig. 5

```
┌──────────────────────────────────┐
│      provide personal data storage │
│   device to an interface peripheral to a │
│  computer in communication with a network │
└──────────────────────────────────┘
                    │
                    ▼
┌──────────────────────────────────┐
│  automatically determine user authorization │
│  methods using data stored on a portable data │
│  storage device peripheral to the computer │
│      in communication with a network │
└──────────────────────────────────┘
                    │
                    ▼
┌──────────────────────────────────┐
│   automatically determine at least an available │
│   user information entry device in communication │
│ with the computer in communication with a network │
└──────────────────────────────────┘
                    │
                    ▼
┌──────────────────────────────────┐
│  determine user authorization methods each │
│   requiring data only from available user │
│        information entry devices │
└──────────────────────────────────┘
                    │
                    ▼
┌──────────────────────────────────┐
│   receive user authorization information in │
│     accordance with a determined user │
│          authorization method │
└──────────────────────────────────┘
                    │
                    ▼
              ╱──────────╲
            ╱      is      ╲
           ╱      user      ╲
           ╲   authorized?  ╱
            ╲              ╱
      No      ╲──────────╱
                    │ Yes
                    ▼
┌──────────────────────────────────┐
│    access security data stored on the │
│       portable data storage device │
└──────────────────────────────────┘
```

Fig. 6a

```
┌─────────────────────────────────────┐
│  automatically determine user authorization │
│  methods using data stored on a key server in │
│  communication with a computer │
│  in communication with a network │
└─────────────────────────────────────┘
                    │
                    ▼
┌─────────────────────────────────────┐
│  automatically determine at least an available │
│  user information entry device in communication │
│  with the computer in communication with a network │
└─────────────────────────────────────┘
                    │
                    ▼
┌─────────────────────────────────────┐
│  determine user authorization methods each │
│  requiring data only from available user │
│  information entry devices │
└─────────────────────────────────────┘
                    │
                    ▼
┌─────────────────────────────────────┐
│  receive user authorization information in │
│  accordance with a determined user │
│  authorization method │
└─────────────────────────────────────┘
                    │
                    ▼
             ◇ is user authorized? ◇
      No                          Yes
                    │
                    ▼
┌─────────────────────┐
│  access key data │
│  stored on the │
│  key server │
└─────────────────────┘
```

Fig. 6 b

Insert blank portable data storage device
in an interface peripheral to a computer
in communication with a network

↓

establish secure communication
session from the portable data
storage device to the key server

↓

transfer secure key data via the secure
communication session from the key
server to the portable data storage device

↓

store the transferred secure key data within
the memory means of the portable data storage device

↓

remove portable data storage device
from the interface peripheral to a computer
in communication with a network

↓

resume normal operation using
the portable storage device
for authorization purposes

Fig. 7

DECLARATION FOR PATENT APPLICATION

As below named inventors, we hereby declare that:

Our residence, post office addresses and citizenship are as stated below next to our names, **Laurence Hamid and Robert D. Hillhouse.**

We are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled

FLEXIBLE METHOD OF SECURITY DATA BACKUP

We hereby state that we have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of the Federal Regulations, S1.56(a).

We hereby appoint the following agent to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Gordon Freedman   **Regn. No: 41,553**
At telephone number: **(613) 274-7272**

Address all correspondence to: **Gordon Freedman**
                                  Freedman & Associates
                                  117 Centrepointe Drive, Suite 350
                                  Nepean, Ontario
                                  Canada
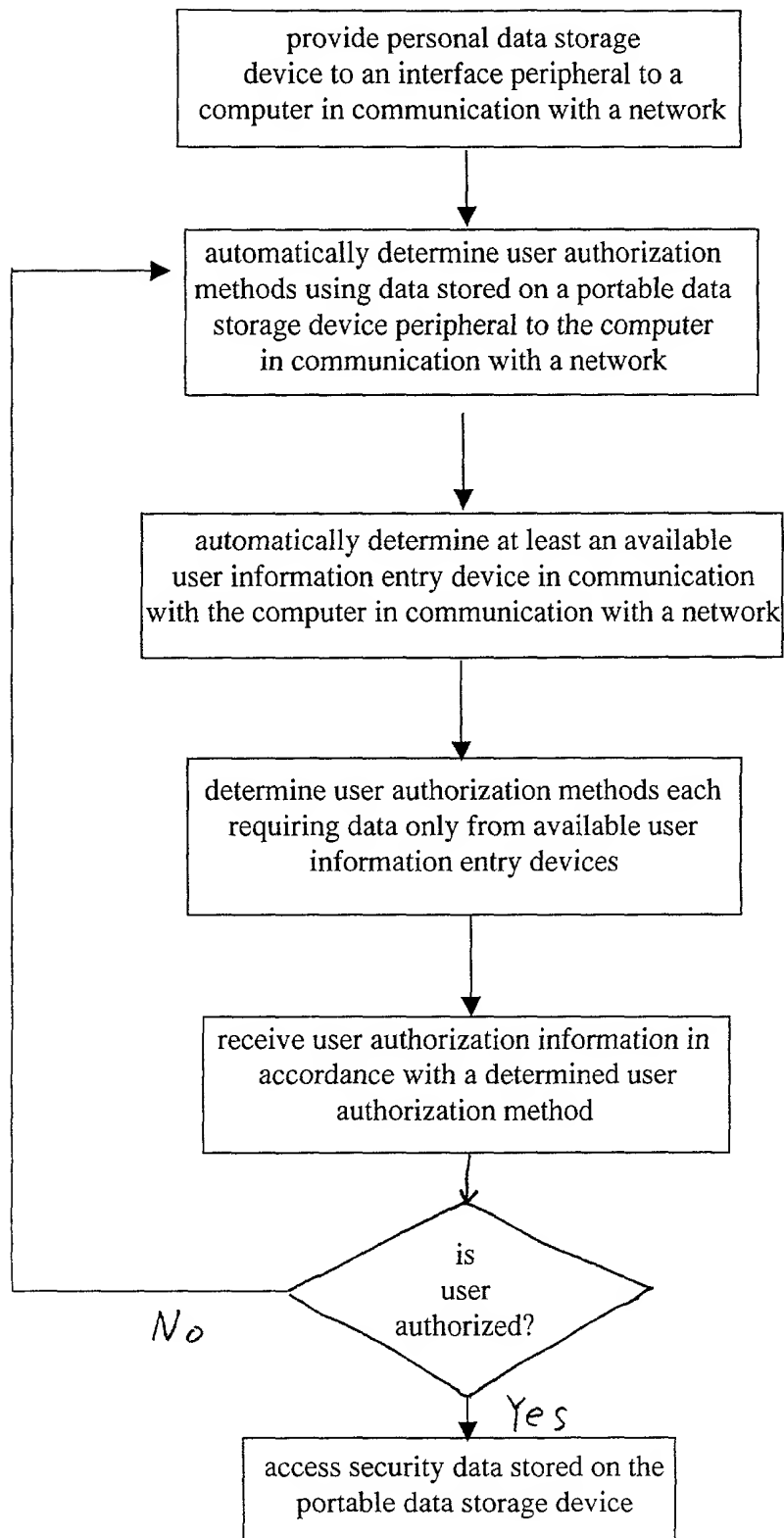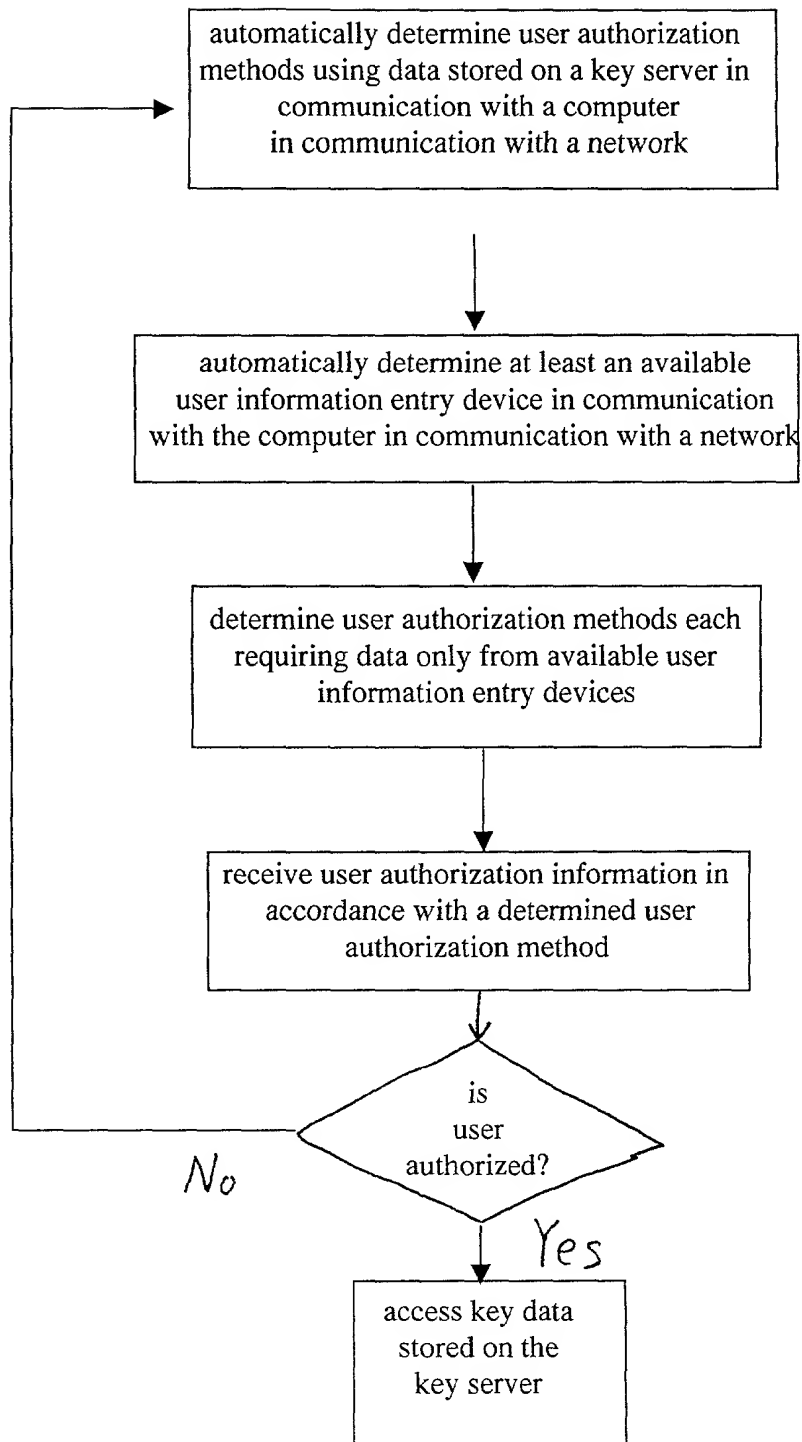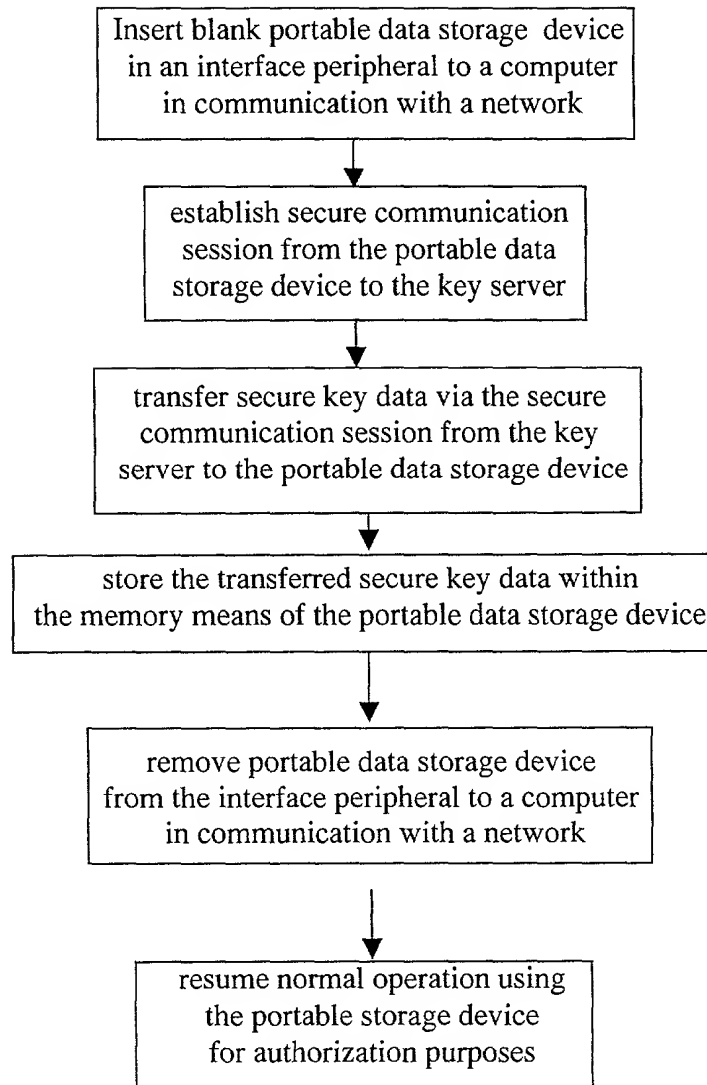   **K2G 5X3**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: **Laurence Hamid**

Inventor's signature: _Laurence Hamid_   Date: _March 8, 2000_

Residence: **124 Pretoria Avenue, Ottawa, Ontario, Canada, K1S 1W9**

Post office address: **As Above**

Citizenship: **Canadian**

Full name of second inventor: **Robert D. Hillhouse**

Inventor's signature: _RDHillhouse_   Date: _March 15, 2000_

Residence: **245 Irving Place, Ottawa, Ontario, Canada K1Y 1Z9**

Post office address: **As Above**

Citizenship: **Canadian**